This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) An apparatus ~~In a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a system for providing virus protection~~ comprising:

~~a gateway coupled between the first network and the destination, which includes~~

a firewall configured to:

receive ~~, which receives the~~ data packets over a first network; ~~, and~~

~~virus scanning engine, coupled to the firewall, which receives the data packets after reception by the firewall, tests the data packets, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested and contain a virus, wherein the firewall~~

classify ~~classifies~~ the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus;

forward ~~and forwards~~ the data packets of the first type to a ~~the~~ destination without testing by a ~~the~~ virus scanning engine; and

forward ~~forwards~~ the data packets of the second type to a ~~the~~ virus scanning engine for testing ~~thereof~~.

2-3. (Canceled)

4. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, wherein~~:~~ the classifying comprises determining that data packets of the first type contain real time data.

5. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim ~~4~~3, wherein~~:~~ the classifying comprises determining that data packets of the first type are part of an audio or video data stream~~contain real time data~~.

6. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, wherein~~: the virus scanning engine, when a virus is detected, alerts the firewall that a virus has been detected which,~~ the firewall is configured to stop reception of a data stream containing the data packets in response to ~~the~~ an alert from the virus scanning engine~~, stops reception of a data stream containing the data packets~~.

7-10. (Canceled)

11. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, further comprising ~~wherein:~~a buffer configured to store ~~which stores~~ the data packets of the second type while the virus scanning engine is testing ~~processing~~ the data packets ~~of the second type~~ to detect a virus.

12-31. (Canceled)

32. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, wherein~~:~~ the firewall is configured to receive from a packet classification database~~, coupled to the firewall, which provides~~ information defining ~~to the firewall which defines~~ the first and second types of data packets~~;~~

~~and a virus detection database, coupled to the virus scanning engine, which provides programming controlling the testing of the data packets of the second type by the virus scanning engine~~.

33. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 32, further comprising: ~~4 wherein:~~

~~a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and~~

a virus scanning engine configured to receive from a virus detection database~~, coupled to the virus scanning engine,~~ programming information ~~which provides programming~~ controlling the testing of the data packets of the second type by the virus scanning engine.

34. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, further comprising: ~~7 wherein:~~

~~a packet classification database, coupled to the firewall, which provides information to the firewall which defines the first and second types of data packets; and~~

a virus scanning engine configured to receive from a virus detection database~~, coupled to the virus scanning engine,~~ programming information ~~which provides programming~~ controlling the testing of the data packets of the second type by the virus scanning engine.

35-39. (Canceled)

40. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, further comprising a ~~wherein: the~~ virus scanning engine~~, upon detection of a virus in the data packets,~~ configured to alert ~~also alerts~~ the destination upon detection of a virus in the data packets~~that a virus has been detected~~.

41. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1 wherein~~:~~ the destination is a local area network.

42. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1 wherein~~:~~ the destination is a personal computer.

43. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, wherein~~:~~ the destination is a second network.

44. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, wherein~~:~~ the first network is a wide area network.

45. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 44, wherein~~:~~ the wide area network is the Internet.

46. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, wherein~~:~~

~~the first network is the Internet; and~~

the destination comprises an Internet service provider configured to connect ~~coupled~~ to a ~~the~~ gateway, a modem configured to connect ~~coupled~~ to the Internet service provider, and one of a local area or personal computer configured to connect ~~coupled~~ to the modem.

47. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 1, further comprising a ~~wherein:the~~ virus scanning engine configured to decode ~~decodes~~ the data packets during the testing of ~~determination if~~ the data packets ~~contain a virus~~.

48. (Currently Amended) The apparatus of ~~A system in accordance with~~ claim 47, wherein~~:~~ the virus scanning engine is configured to function ~~functions~~ as a proxy for a destination processor configured to receive ~~which receives~~ the data packets.

49. (Currently Amended) A ~~In a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination, which includes a firewall and a virus scanning engine, said firewall receiving the data packets, a~~ method comprising:

receiving ~~the~~ data packets ~~at the firewall~~;

classifying the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and a second type which can contain a virus;

transmitting the received data packets of the first type to a ~~the~~ destination without testing by a virus scanning engine; and

transmitting the received data packets of the second type ~~from the firewall~~ to a ~~the~~ virus scanning engine for testing~~;~~

~~testing the data packets with the virus scanning engine; and~~

~~transmitting from the virus scanning engine any data packets which are tested by the virus scanning engine to not contain any virus to the destinationand the discarding any data packets which are tested to contain a virus~~.

50. (Currently Amended) A computer program stored on a storage medium comprising computer executable instructions for performing a method comprising:

~~for use in a virus scanning engine in a communication system including at least a first network coupled to a destination to which transmissions of data packets are made from the first network to the destination, a gateway coupled between the first network and the destination, which includes a firewall and the virus scanning engine, coupled to the firewall, said firewall~~

receiving ~~the~~ data packets~~;~~, ~~the virus scanning engine receiving the data packets after reception by the firewall, passes any data packets, which are tested to not contain a virus to the destination and discards any data packets which are tested to contain a virus, said firewall~~

classifying the received data packets based on the contents of the data packets into packets of a first type that cannot contain a virus and a second type that can contain a virus; ~~and~~

transmitting ~~forwards~~ the data packets of the first type to a ~~the~~ destination without testing by a ~~the~~ virus scanning engine; and

transmitting ~~forwards~~ the data packets of the second type to a ~~the~~ virus scanning engine for testing ~~thereof, the computer program when executed causing the virus scanning engine to execute at least one step of:~~

~~testing the data packets for the presence of a virus~~.

51-52. (Canceled)

53. (Currently Amended) A computer program in accordance with claim 50, ~~51,~~ wherein~~:~~ the classifying comprises determining that data packets of the first type contain real time data.

54. (Currently Amended) A computer program in accordance with claim 50, wherein:

the computer program when executed causes ~~the virus scanning engine, when a virus is detected, to alert the firewall that a virus has been detected which, in response to the alert, controls the firewall to stop~~ reception of a data stream containing the data packets to be stopped in response to an alert from the virus scanning engine.

55. (Canceled)

56. (New) A computer program in accordance with claim 50, wherein the method further comprises receiving from a packet classification database information defining first and second types of data packets.

57. (New) A computer program in accordance with claim 53, wherein the classifying further comprises determining that data packets of the first type are part of an audio or video data stream.

58. (New) The method of claim 49, wherein the classifying comprises determining that data packets of the first type contain real time data.

59. (New) The method of claim 58, wherein the classifying further comprises determining that data packets of the first type are part of an audio or video data stream.

60. (New) The method of claim 49, further comprising receiving information from a packet classification database, said information defining the first and second types of data packets.

61. (New) The method of claim 49, wherein the classifying is performed by a firewall.

62. (New) Apparatus, comprising:

a processor configured to control at least some operations of the apparatus;

memory storing computer executable instructions that, when executed by the processor, cause the apparatus to:

receive data packets;

classify the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and a second type which can contain a virus;

transmit the received data packets of the first type to a destination without testing by a virus scanning engine; and

transmit the received data packets of the second type to a virus scanning engine for testing.

63. (New) The apparatus of claim 62, wherein the classifying comprises determining that data packets of the first type are part of an audio or video data stream.